Certificate Repository Security Discussions

Sandi Miklos

National Security Agency

8 October 1998

samiklo@missi.ncsc.mil

General Statement

- The contents of this briefing are Unclassified
- The opinions expressed are not necessarily those of my employer
- Security is not an unnatural act!

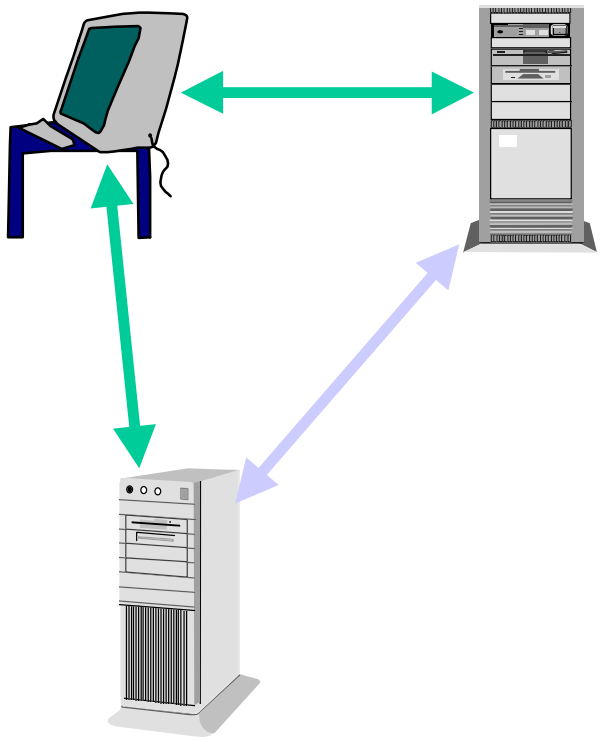
Briefing Outline

- Philosophy of Protection
- Generic Environment
- Threats
- Requirements
- Protocol Options
- Summary

Philosophy of Protection

- Laws, rules, regulations
  - Define operating environment
  - Make assumptions about intended usage
- Derive security objectives
  - Threats, policies, assumptions
    - Computing-base implemented policies
    - Imposed on entities in environmental policies
- Define protection mechanisms
  - Enforced by computing base
  - Enforced by environment

Repository Communications Protocol(s)



Client Access Protocol(s)

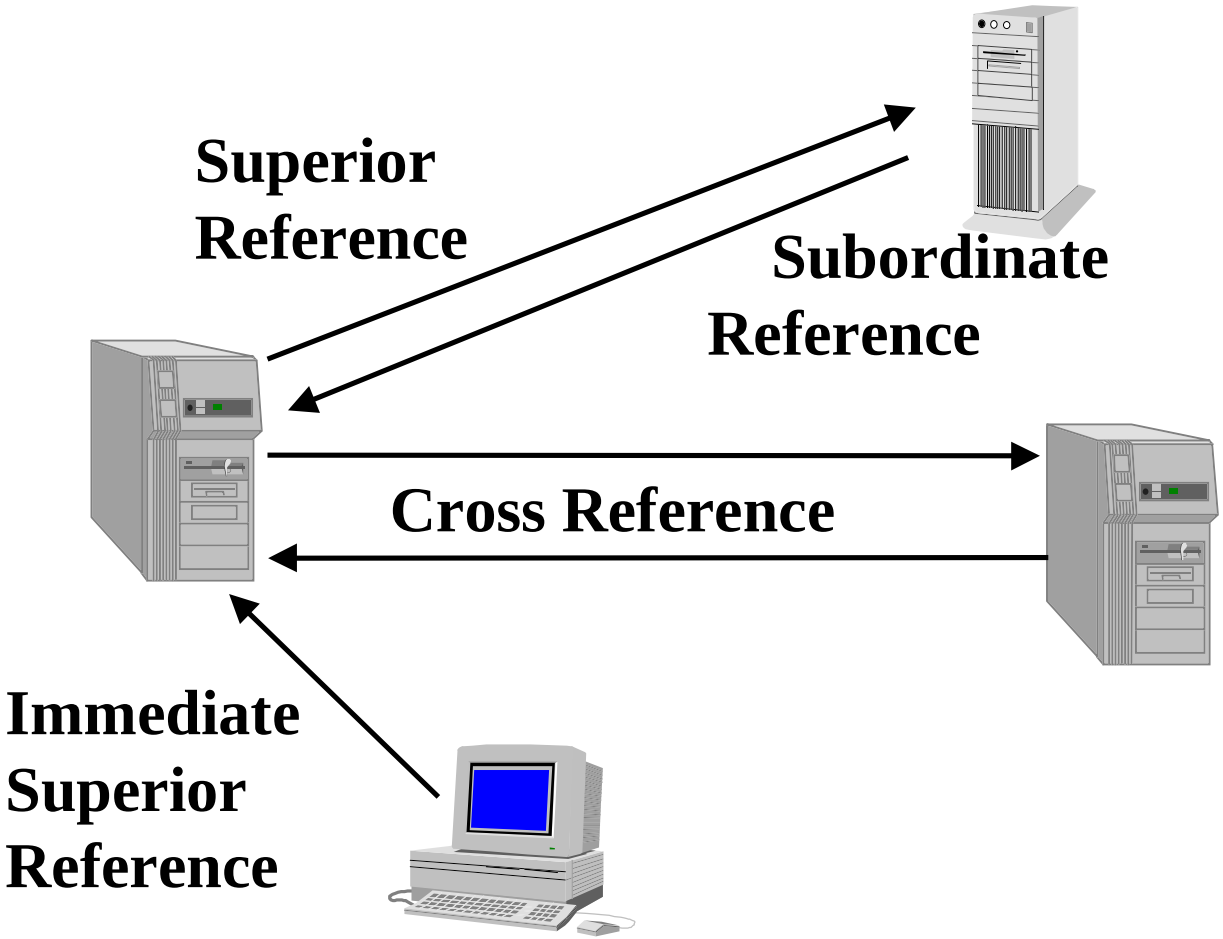
-Operators

-Administrators*

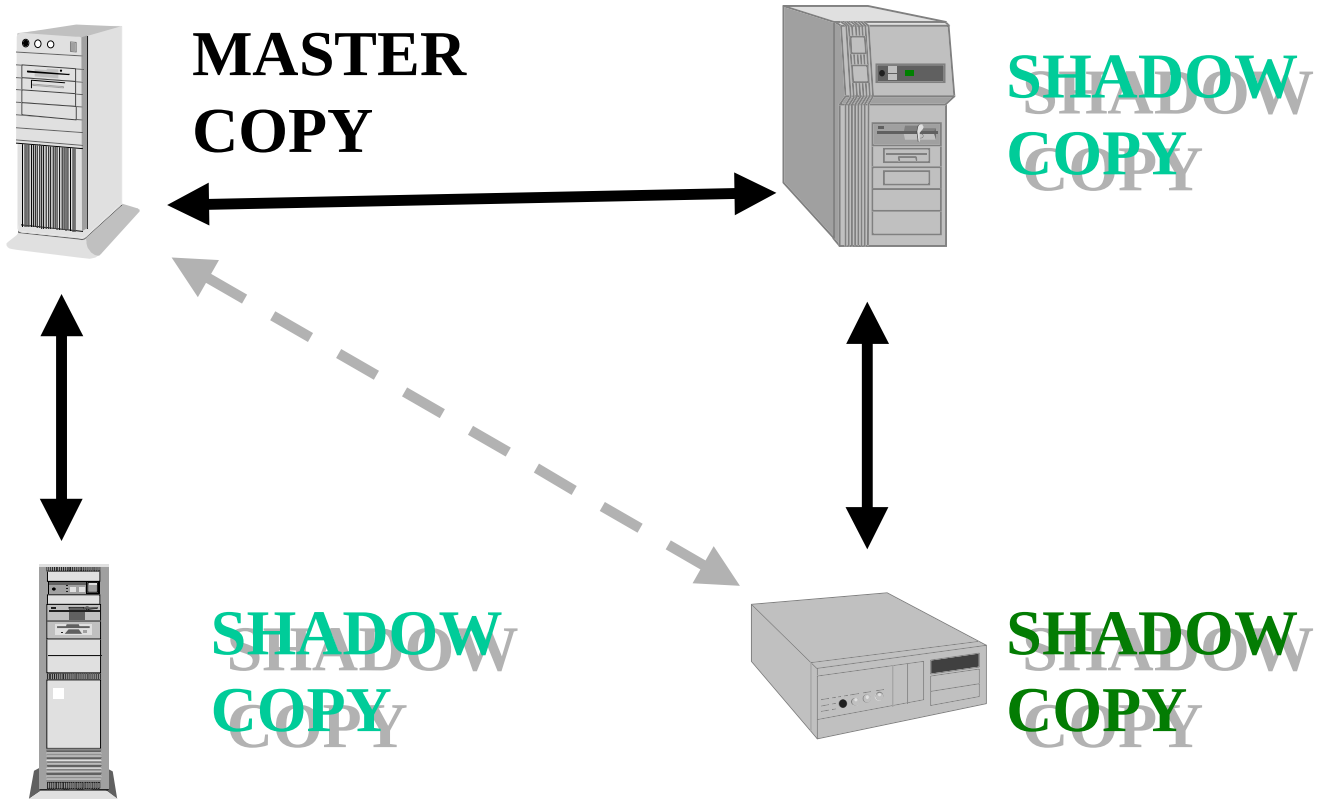
-Maintenance

-General access

Navigating the Distributed System



Data Replication



Threat Assessment

- Threat categories
  - Replay
  - Manipulation
  - Masquerade
  - Data modification
  - Denial of service

Threat Assessment

- Threats not covered in this briefing
  - Eavesdropping
  - Traffic analysis
  - Directory as a covert channel

Threat Agents

- Operators acting as authority
  - Exceed rights
  - Incorrect performance of tasks
  - Attack assets such as sensitive stored data, software and hardware
- Users
  - Bypass and exploit weaknesses in access controls
  - Impersonate operators and manipulate management services

Means of Attack

- Replay
  - Threat agent (TA) has substituted information with ‘old’ information obtained from a previous transaction
- Manipulation
  - TA alters information legitimate user reads or writes to the directory
- Masquerade
  - TA impersonates either legitimate user or a DSA

Means of Attack

- Data modification
  - TA modifies entry information (modifies, deletes or adds attributes or entries, or alias information)
- Denial of service
  - TA prevents legitimate users from accessing either the repository or information in it
  - TA consumes repository resources

Repository Functional Requirements

- Publish and provide access to:
  - User public key certificates
  - CA public key certificates
  - CA cross certificates
  - Certificate revocation lists (CRL)
  - Authority revocation lists (ARL)
  - Other related PKI attributes (e.G. Policy)

Repository Functional Requirements

- Securely maintain operator information
  - Separation by role
    - Administrators*
    - Maintenance
  - Authentication private key (DSA ‘component’)
  - Storage of operator pins
- Securely maintain audit information
  - Support alarm conditions
  - Permit threshold adjustment
  - Restrict access to audit information

Minimum Repository Security Requirements

- Authenticate user and operator identities
- Maintain integrity of information stored in repository
- Enforce access control for data
  - Write / modify access to PKI-related data restricted to CAs
- Ensure availability of information
- Determine if confidentiality is required

Authentication

- Anonymous
- Simple
  - Name and password (in the clear)
- Protected simple
  - Name and hash of password
    - Limited protection against masquerade; no protection against replay
- Strong authentication
  - One or two-way
  - Continuous / session

Strong Authentication

- Agree on protocol elements and algorithm parameters
  - Sdn.705 - x.500
  - Consider impact of numerous permutations of authentication tokens
- Algorithm agility
  - Development of a security toolkit functionality
  - Multiple hash/signature algorithms
- Address DSA credential management
  - Creation
  - Storage in repository
  - Revocation

Integrity

- In transmission
  - Each operation argument, result and error (transaction) may be signed or unsigned
- In storage
  - Certificate-related information (certificates, crls, arls, etc.) are signed objects

Integrity

- In transmission
  - Evaluate each operation argument, result and error and determine the protection to be applied (signed, unsigned)
    - Evaluate risk to private key
  - Consistent repository quality-of-protection across domain
- In storage
  - Evaluate schema to identify those attributes that may require integrity
  - Consistent encoding across domain
    - Includes all components that “touch” repository and may have to validate signature

Example Quality of Protection Agreement

See handout

Access Control

- Determine
  - Authentication level mapped to user and operation requested
  - Create list of users and permissions granted or denied
    - Specify either list of users and their permissions or list of permissions and users who have these permissions
  - Distribution of access control information (ACI) to all repositories in domain
    - Consistent ‘end result’ across all implementations of an access control decision function

Access Control

- User PKI information should be readable by all entities with no authentication required
  - Critical to retrieval of CRLs
- Operators / administrators should have separate access to operational information
  - ACI example
- CAs should have separate access to manage PKI-related user information
  - Modify RDN restricts CAs from creating entries

Identification Tag: "Public access control"
Precedence: *n*
Authentication Level: none
User Class: all users

Protected Items:	Attribute Type {common name, telephone number, fax number, object class},
	All Attribute Values {common name, telephone number, fax number, object class},
Permissions:	grant read, grant filterMatch, grant discloseOnError
Protected Items:	Entry
Permissions:	grant browse, grant read, grant returnDN, grant discloseOnError

This ACI grants public access to a selected set of attributes in an entry by allowing read and search access to the telephone and fax number, common name, distinguished name and object class of one or more entries and returns useful diagnostics if the users have errors in their requests.

*REPRINTED FROM "UNDERSTANDING X.500" D. Chadwick

Availability

- 24 x 7
  - Manage knowledge information to include primary and backup references
    - Client configuration
    - Server knowledge
  - Back up database every 12 hours
  - Offsite backup every 24 hours

Example Working Group

- Agreement, in principle, to the following security services and mechanisms apropos to directory interactions:
  - Strong authentication between DSAs
  - Strong authentication for all modify operation binds (requires prior knowledge of that function)
  - No authentication required for read operations (required to retrieve CRLs
  - Digitally signed modify operations (arguments - 1993 protocol; responses and errors - 1997 protocol)

Repository Protocol Options

- X.500 based
- LDAP based (V2 / V3)
- Other
  - HTTP / web mechanism
    - Simple but not integrated with applications and not as fully defined as X.500 or LDAP based options
  - Proprietary database solutions
    - Non-interoperable
  - Application-specific repository solutions
    - No standard interface to PKI

Authentication

- LDAP v3
  - Supports two SASL authentication mechanisms
    <Draft-ietf-ldapext-x509-sasl-00.Txt>
    - Protected password
    - Strong
  - Specific authentication methods identified
    <Draft-ietf-ldapext-authmeth-02.Txt>)
  - LDAP V3 extensions for transaction layer security (TLS)
    <Draft-ietf-ldapext-ldapv3-tls-02.Txt>
    - Granularity of role-based access control?

Authentication

- X.500
  - Strong authentication (public key based) completed in 1988
  - Strong authentication possible on all X.500 protocols (client/server and server/server)
  - Algorithm independent

Integrity

- LDAP standards activity recently initiated
  - Allows protocol operations to be signed
  - Based on S/MIME

  <Draft-ietf-ldapext-sigops-02.Txt>
- X.500
  - 1988
    - Signed operations permitted - merged search results excluded
  - 1997
    - Signed errors and null results
    - All protocols include signed operations

Access Control

- Recent ldapv3 standards activities:
  - Draft access control model available

    <Draft-ietf-ldapext-acl-model-00.Txt>
  - Draft access control requirements available

    <Draft-ietf-ldapext-acl-reqts-01.Txt>
  - Not certain how closely LDAP access control will replicate that defined in X.500

Access Control

- X.500 completed in 1993
  - Protected item
    - Subtree, an entry or an attribute value
  - User class
    - All users (DN of the user is DN of entry)
    - Name (list of users by DN *restricted to access control inner areas)
    - User-group (list of named groups of users *restricted to local knowledge)
    - Subtree (each user's DN falls into the identified subtree)

Access Control

- Permissions
  - Map to operations
    - Read, browse, modify, import, export, etc
  - Defined at entry or attribute level
- Precedence
  - Governs order in which distinct access control statements are applied, if more than one statement applies to an entry. Higher values prevail
- Authentication levels
- Does not address contextual information

Organizational Security Policy

- Provide users with description of measures taken to ensure security
- Restrict direct access to properly I & A'd operators
- Record security-relevant events
  - Detect potential attack / misconfiguration
  - Hold users / operators accountable

Summary

- Use threat assessment, operational policies and assumptions to determine your security objectives for the repository
  - Map this back to the equivalent results from the CA study
- Derive security functions
  - Allocate to computing base or environment

Summary

- Derive assurance requirements
  - For Federal PKI as a whole
  - Refine for individual elements of FPKI
- Ensure that appropriate training and testing is developed and occurs